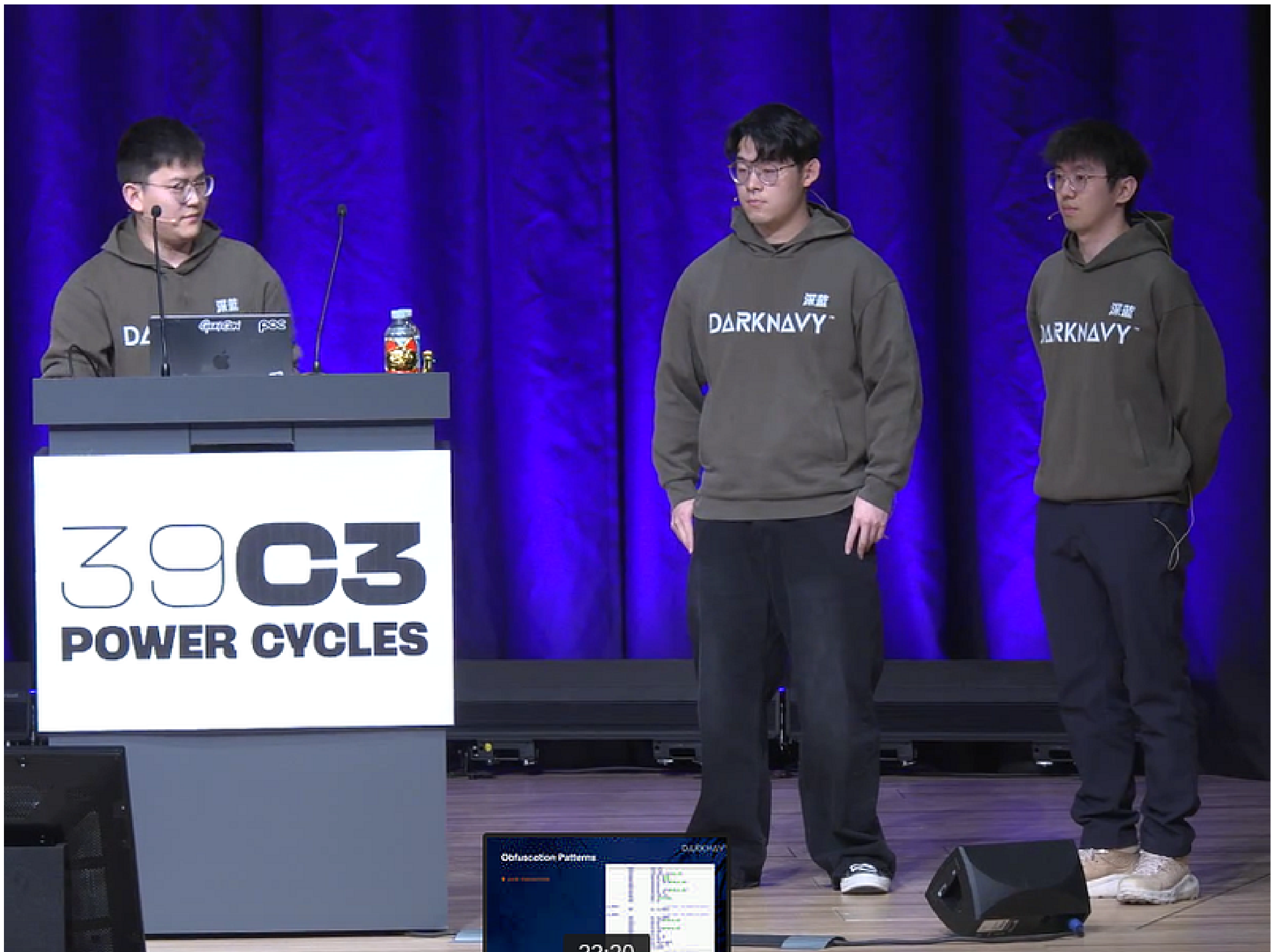
Cassandra Crossing 654/ 39C3: Il kit di sviluppo per Skynet

(654)—Al Chaos Communication Congress di Amburgo tre ragazzi raccontano come hanno preso il controllo di un robot umanoide. Al loro…

Cassandra Crossing 654/ 39C3: Il kit di sviluppo per Skynet



by Chaos Computer Club e.V

(654)—Al Chaos Communication Congress di Amburgo tre ragazzi raccontano come hanno preso il controllo di un robot umanoide. Al loro splendido talk Cassandra aggiungerà solo il suo piccolo contributo di paranoia.

28 dicembre 2025—Non avendo potuto recarvisi di persona, Cassandra si è valsa della mai abbastanza lodata abitudine che i convegni hacker hanno di fare streaming in diretta e di pubblicare video integrali degli interventi.

Ne ha quindi approfittato per godersi (si fa per dire—vedremo perché) il talk "*Skynet Starter Kit: From Embodied AI Jailbreak to Remote Takeover of Humanoid Robots*", presentato da Shipei Qu, Zikai Xu e Xuangan Xiao dell'organizzzazione Darknavy al convegno 39C3 di Amburgo, organizzato dal Chaos Computer Club.

“*Una scatola di montaggio per Skynet: dalla violazione di IA incorporate fino alla conquista del controllo remoto di robot umanoidi*”

Se il titolo vi ha fatto salivare, potete smettere di leggere e godervi la registrazione video completa, disponibile appena due ore dopo il talk,.

In breve: i relatori si sono comprati un robot umanoide, un Unitree G1 prodotto dalla cinese Unitree Robotics, denominazione sotto cui opera la Hangzhou Yushu Technology Co., Ltd., azienda che nel materiale commerciale indica di aver già venduto 50.000 robot.

A causa degli alti costi, il modello Unitree G1 scelto dai relatori di Darknavy è stato il più basico, visto che costava già 20.000 Euro.

La costruzione della serie di robot G1 (a Cassandra vengono i brividi a scrivere come *Susan Calvin*) è modulare; il robot esaminato è dotato di capacità elementari, e può solo essere teleguidato da un operatore umano, tramite un controller che usa un cellulare come schermo, proprio come quelli dei droni. Niente autonomia, quindi.

Nel torace del robot troviamo infatti lo spazio ed i connettori per una scheda “cervello” NVIDIA Jetson Orin, un processore ad alte prestazioni che esegue i programmi più onerosi, come l’interpretazione delle nuvole di punti Lidar ed i modelli IA, che non è ovviamente installata nel modello base.

I nostri “eroi” (termine meritatissimo!) hanno descritto dettagliatamente come hanno potuto prendere, totalmente e da remoto, il controllo del robot, in modo da poterlo guidare al posto del proprietario. Hanno fatto questo passando dai livelli più “elementari” delle funzionalità del robot, quindi probabilmente avrebbero potuto farlo anche sui modelli dotati di autonomia, cioè la versione “EDU” del G1.

“*Com'è accaduto? Di chi è la colpa?*“

No, oggi non scomoderemo l’immortale “V” per banali questioncelle sulla qualità dei prodotti industriali.

E neppure vi racconteremo i dettagli della “campagna di conquista” del robot, che i nostri eroi descrivono benissimo nel loro intervento, tra l’altro in un inglese comprensibilissimo.

Appena due parole meritano le cause delle falle di sicurezza, così gravi ed importanti ma che non meravigliano Cassandra, e non dovrebbero meravigliare nemmeno i 24 informatissimi lettori.

Si tratta infatti semplicemente di “*Business as usual*”. Sono le stesse problematiche, già tante volte raccontate, presenti negli oggetti connessi; nei computer, nelle lampadine ed in tutti gli oggetti IoT, iniziando dai Nabaztag.

Bug arcinoti, che sarebbero evitabili semplicemente spendendo pochi spiccioli nei posti giusti del ciclo di vita del prodotto.

Comunicazioni in chiaro, password note o scritte nel codice, protocolli standard male utilizzati, nessuna protezione da attacchi via radio o via rete, mancato utilizzo dei numerosi meccanismi di sicurezza esistenti nelle componenti hardware e software ma non utilizzati.

Con una eccezione, però; i meccanismi di sicurezza per offuscare il codice al fine di renderne difficilissima la copia, e salvaguardare così la cosiddetta “proprietà intellettuale”, sono, quelli sì, utilizzati in abbondanza.

La sicurezza del prodotto e dei suoi utenti è relegata come sempre accade all'ultimo posto, proprio quello dove poi si iniziano a tagliare i costi per risparmiare.

Riassumendo: all'interno i robot sono costruiti male, proprio come le lampadine, i Nabaztag o le lavatrici. Non a caso al 39C3 è in programma anche un intero laboratorio sull'hacking delle lavatrici.

Ora, il "*povero*" G1 è alto solo 1,30 metri e pesa 35 chili. Non proprio un colosso armato fino ai denti come Terminator. Ma ha muscoli funzionanti e, se guidato con fini malevoli, può essere pericoloso anche lui.

Alcuni robot sono già adesso estremamente veloci e forti, molto più di un essere umano; ma anche i modesti servomotori di un G1, se spinti al massimo, farebbero il loro effetto.

Ci facciamo "ingannare" dagli occhi azzurri, dolci ed ammiccanti dei giocattoli e delle badanti robot che vediamo nelle pubblicità, e ci dimentichiamo invece degli occhi rossi di Terminator. E di cosa un robot malfunzionante o manipolato potrebbe fare.

Concludendo: se il livello con cui si realizzano i robot commerciali è questo, **cosa impedirà al primo malintenzionato di trovarli con Shodan, violarli con Metasploit, attivarli mentre sono alle spalle del loro proprietario, e fargli staccare la testa con solo un veloce fruscio di arti meccanici**?

In questo caso, non sarà necessario ricorrere a Sherlock Holmes od Elijah Baley per capire cosa sia successo; basteranno dei ragazzi di talento, come i nostri relatori, che siano pratici della malarealizzazione degli aggeggi IoT.

Perché i robot umanoidi che a breve troveremo sul mercato avranno mani, braccia e si muoveranno. Saranno forti e veloci, anche quelli che non lo sembrano.

Nel caso che siano realizzati con la stessa incuria delle lampadine IoT e dei robot G1, poco importerà che abbiano persino le *Tre Leggi della Robotica* incise nei loro cervelli. Se potranno essere violati e manomessi ai loro livelli basici con questa semplicità, **qualsiasi programmazione "benevola" potrà essere bypassata**.

Forse sarebbe meglio non averli in giro per casa; trasformare la badante del nonno in un robot assassino potrebbe essere davvero troppo, troppo facile.

Scrivere a Cassandra—Twitter/X—Mastodon
Videorubrica "Quattro chiacchiere con Cassandra"
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero

Cassandra per i posteri: l'archivio su Internet Archive

Licenza d'utilizzo*: i contenuti di questo articolo, dove non diversamente indicato, sono sotto licenza Creative Commons Attribuzione—Condividi allo stesso modo 4.0 Internazionale (CC BY-SA 4.0),* tutte le informazioni di utilizzo del materiale sono disponibili a questo link.

By Marco A. L. Calamari on December 29, 2025.

Canonical link

Exported from Medium on March 30, 2026.